Security Work Group
http://www.nitc.state.ne.us/tp/workgroups/security/index.htm

Tuesday May 6, 2003
10:00 A.M. to Noon
NSOB Conference Room F (Lower Level) – Lincoln, NE

Minutes

A. Participants

Rod	Armstrong	NOL
Allan	Albers	HHSS
Cathy	Danahy	Secretary of State / Records Management
Jerry	Hielen	IMServices
Scott	McFall	State Patrol
Leona	Roach	University of Nebraska
Linda	Salac	HHSS
Steve	Schafer	Nebraska CIO
Ron	Woerner	Department of Roads

A. Discuss Draft Wireless Policy (April 2, 2003, Version)

Discussion included the following changes to the draft document:

1. In the Purpose and Objectives section, make it clear that the Remote Access Guidelines will not take the place of specific procedures of operational entities.
2. Eliminate references to NIST recommendations.
3. Edit the document so that terminology is consistent with voluntary guidelines. Use the word, "should" instead of "must". The exception is that registration of wireless devices connected to the state's network will be mandatory.
4. Clarify the requirements for registration of wireless devices by state agencies.
5. Include a definition of "access point" in the glossary.
6. Include the proposed IMServices "Network Security Standards" in the list of references.

B. Discuss Draft Remote Access Policy (April 3, 2003, Version)

Discussion included the following changes to the draft document:

1. In the Purpose and Objectives section, make it clear that the Remote Access Guidelines will not take the place of specific procedures of operational entities.
2. Delete the language in several places regarding "NIST recommendations".
3. Delete references to other sections in the NIST guidelines for more detail.

C. Discuss Secure Communications Issue

This item was deferred to the next meeting. The NOTES advisory group has been working on certification across NOTES environments. Members of the NOTES advisory group are developing guidelines on what things agencies must do to provide secure e-mail on different systems. One issue that is not resolved is who will monitor for compliance. This topic will be deferred to the next meeting for further discussion.

D. Briefing on National Cyber Security Strategy

Ron Woerner gave a presentation on the National Strategy to Secure Cyberspace (February 14, 2003). A copy of the strategy is available at: http://www.whitehouse.gov/pcipb/. The purpose of the strategy

is to encourage people, businesses, and governments to secure the portions of the cyberspace that they own, operate, control or interact with. Strategic objectives include:

- Prevent cyber attacks against America's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks that do occur.

The strategy includes five priorities:

- A national cyberspace security response system;
- A national cyberspace security threat and vulnerability reduction program;
- A national cyberspace security awareness and training program;
- Security government's cyberspace;
- National security and international cyberspace security cooperation.

One element of the security awareness program is Microsoft's "StaySafeOnline campaign (http://staysafeonline.org/). Training cybersecurity professionals and promoting cybersecurity certifications are other elements of the security awareness strategy.

Security government's cyberspace has several components, including:

- Fostering a marketplace for more secure technologies through procurement policies;
- Continually assess threats and vulnerabilities to cyber systems;
- Authenticate and maintain authorized users of cyber systems;
- Encourage state and local governments to establish information technology security programs and participate in information sharing and analysis centers (ISACs) www.ciao.gov/industry/isac.html .

The national strategy adopts some common sense measures, while mandating the federal government to secure itself. It also leverages several current security initiatives. These include the OECD security guidelines (http://www.oecd.org/pdf/M00033000/M00033182.pdf), Technet CEO Cybersecurity Task Force (http://www.technet.org/press/Press_Releases/?newsReleaseId=1746), and Microsoft's Trustworthy Computing Initiative. (Microsoft's Security website is http://www.microsoft.com/security/. Their white paper on Trustworthy computing is at http://www.microsoft.com/presspass/exec/craig/10-02trustworthywp.asp.

E. Update on Security Initiatives

1. Jerry Hielen gave an update on the Directory Services Project. An ad hoc group is working through a range of issues that must be decided as part of configuration and set up. The procedure for resetting passwords is one example.
2. The external intrusion security assessment is underway. Phase I (discovery) is done, and OmniTech is starting work on Phase II (vulnerability scanning).
3. IMServices has prepared a draft set of network standards that apply to agencies with a connection to the state's interagency network. The document incorporates good network management practices pertaining to physical security, operating system installations, firewalls, and other topics. The document includes a provision that "IMServices may disable the network port of the offending server … in the event that one or more (or an agency's) servers is compromised and negatively impacting other servers or network performance." Discussion indicated that IMServices would only disconnect the server from the network without needing to have system administrator access to the server.
4. The cost for web-based security training is about $6 per person per year, if we meet a certain threshold. Several agencies are determining whether they want to participate.

5. NEMA has included continuity of operations / continuity of government in the state's application for federal Homeland Security funding.

F. Other Security Issues

1. Draft SPAM Control Standards (future discussion)
2. Regional Computer Incident Response Teams (future discussion)
3. Future activities of the Security Work Group. In addition to working on security guidelines, there is interest in using this group for information sharing on a broad range of security issues. Examples include:
    - Create a high level strategy for improving security, with tactical steps for implementation;
    - Conduct an audit against actual security policies and practices;
    - Set minimum standards for state government and work for voluntary compliance;
    - Discuss shared problems and issues, rather than only working on guidelines;
    - Track multiple federal security requirements from HIPAA, IRS, Cyber Strategy.

G. Next Meeting Dates – to be announced

Potential topics for the next meeting include secure communications, SPAM control, regional CIRT, minimum standards and strategic plan, and information sharing.

Security Newsletters And Alerts

SANS

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 156,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community.

SANS NewsBites - weekly

NewsBites saves you from having to read every trade publication and newspaper to find the key security stories. It keeps up with everything going on in the computer security world. A dozen or two articles, each just one, two, or three sentences in length, elaborate a URL that points to the source of the detailed information.
Review samples.

Critical Vulnerability Analysis Newletter - weekly

The new Critical Vulnerability Analysis report is delivered every Monday morning. It focuses on the three to eight vulnerabilities that matter, tells what damage they do and provides data on the actions 15 giant organizations took to protect themselves.
Review samples.

Security Alert Consensus (SAC) - weekly

One definitive weekly summary of new alerts and countermeasures each week with announcements from: SANS, CERT, the Global Incident Analysis Center, the National Infrastructure Protection Center, the Department of Defense, Security Portal, Ntbugtraq, Sun, Microsoft and several other vendors. When you subscribe, by selecting only the operating systems you support, you will receive a version of Security Alert Consensus tailored and customized to your needs: just pick the operating systems you want included in your customized weekly digest.
Review samples.

For a free subscription, (and for free posters) visit http://www.sans.org/sansnews/

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings - DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications - DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other Publications DHS/IAIP Daily Reports Archive - Access past DHS/IAIP Daily Open Source Infrastructure Reports